Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

L'archivage face à l'électronique ou comment éviter l'amnésie collective ? Le point de vue du juriste

Poullet, Yves

Publication date:
2002

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Poullet, Y 2002, *L'archivage face à l'électronique ou comment éviter l'amnésie collective ? Le point de vue du juriste*..

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 23. Apr. 2024

L'archivage face à l'électronique

ou

Comment éviter l'amnésie collective
– le point de vue du juriste –

Yves Poullet
Doyen de la Faculté de droit de Namur
Directeur du CRID des FUNDP
yves.poullet@fundp.ac.be
http://www.droit.fundp.ac.be/crid

1. L'archivage au sens étroit du terme, c'est-à-dire l'activité relative à la production, l'exploitation et à la conservation des « archives définitives »[1], c'est-à-dire de « l'ensemble de documents, qui ne présentant plus d'utilité administrative ou juridique pour le formateur d'archives, gardent une valeur probatoire justifiant leur conservation sans limitation de durée »[2] participe au « devoir de mémoire » et engage la responsabilité du politique et de l'administration face à l'histoire. L'archivage représente en ce sens une valeur essentielle pour nos démocraties[3].

2. L'utilisation de supports électroniques pour la réalisation de cet archivage tend à se multiplier soit parce que l'original est désormais électronique (ainsi, l'e mail ou le message internet émis par une administration ou un ministre à propos d'un problème quelconque) soit parce qu'à l'original papier on préfèrera substituer une copie électronique pour des raisons claires de diminution des coûts de stockage et d'efficacité plus grande dans le classement et donc dans le repérage des documents ainsi stockés[4].

Cette utilisation soulève donc nombre d'espoirs : aux kilomètres de dossiers que peuvent représenter les archives de la justice, parmi lesquels un chercheur ne retrouvera qu'au prix de maints aller-retour les documents souhaités, se profile l'espoir de la manipulation aisée quelques DvD-Rom[5] dont l'indexation ou la recherche par mots voire par contexte permettront l'exploitabilité aisée des documents archivés.

Elle engendre également l'inquiétude. On évoque à cet égard les premiers exemples d'archivages électroniques qui, opérés sur des supports à durée de péremption limitée et incompatibles avec le processus de nouvelle génération, sont définitivement devenues obsolètes[6] et par conséquent entraîné la perte de milliers de documents. Les risques de

---

[1] La notion d"archive définitive" s'oppose à celle d' "archive courante » (c'est-à-dire, d'un document d'utilisation courante pour l'activité des personnes les ayant produits ou reçus) et à celle « d' archive intermédiaire », document conservé pour des raisons administratives ou juridiques.

[2] Ces définitions sont tirées de l'avant-projet de loi relative aux Archives, préparé par les SSTC et en discussion au moment du congrès franco-belge des archivistes, pour lequel ce texte a été préparé.

[3] "Considérant qu'un pays n'accède pleinement à la démocratie que lorsque chacun de ses habitants dispose de la possibilité de connaître de manière objective les éléments de son histoire » (Préambule de la Recommandation n° R (2000) 13 du Comité des Ministres aux Etats membres sur une politique européenne en matière de communication des archives) Texte disponible sur le site du Conseil de l'Europe http://www.coe.fr/cm/ta/rec/2000/f2000r13.htm

[4] « Contrairement au support papier, le support électronique permet un accès rapide à des données correctement indexées. Des robots se chargent de récupérer la bonne cartouche dans une véritable bibliothèque électronique, et de la placer sur un lecteur libre, et ce, dans un laps de temps sans comparaison avec celui que mettrait un employé pour parcourir les galeries infinies des étagères poussiéreuses où s'entassent des montagnes de dossiers. Symétriquement, à l'heure où les documents utilisés dans la vie de l'entreprise prennent de plus en plus la forme numérique, l'archivage de ceux-ci sous la même forme en est facilité. Un programme automatisé permettrait en effet d'archiver automatiquement un document à la fin de son cycle d'exploitation » (T. Lieutenant et S. Marin, Archivage et horodatage de documents électroniques, Mai 2000, document disponible sur le site du CRID http://www.crid.be à la rubrique e justice (documents disponibles).

[5] IBM propose des solutions de stockage allant jusque 14,4 To de données compressées. Un simple DvD-Ram de 12 cm est susceptible de stocker plus ou moins 5,4 GO de données, un DvD-Rom, plus ou moins 18 GO de données. Le premier disque dur d'IBM en 1956, avait une densité de stockage de 2 kbits/pouce, à comparer avec les 5,7 Gbits/pouce atteints aujourd'hui (on a atteint 20 Gbits en 1999, en laboratoire), le taux de transfert passant de 70 kbits/sec à 118 Mbits/sec !

[6] C'est un lieu commun : le materiel informatique est lui aussi frappe d'obsolescence à un rythme pour le moins rapide, bien que les choses évoluent moins vite dans les grands centres informatiques que pour les produits destinés au grand public. Cependant, l'évolution est inéluctable. Citons à titre d'exemple les disquettes les disquettes 5 " ¼ d'il y a moins de 10 ans, ou les disques durs de la même époque inutilisables sur les ordinateurs

manipulation des données contenues sur les supports sont également soulignés. Bref, tout, loin de là, n'est pas rose au pays de l'électronique[7].

3. L'abord par le juriste du phénomène de l'archivage électronique soulève donc pour le juriste une première question : la définition des conditions d'une conservation fiable dans l'environnement électronique. Comment garantir la stabilité des supports, la lisibilité et l'intégrité des contenus ?

Au-delà de cette première question, le juriste se trouvera confronté à une double exigence qui, à certains égards, peut se révéler contradictoire : le droit à la transparence de l'action administrative implique – et la loi du 10 juillet 1994 le consacre – le droit d'accès des citoyens non seulement aux archives courantes dites « vivantes » mais également à celles « intermédiaires » et enfin à celles « définitives » dites « mortes » qui sont l'objet de notre propos. Ce droit d'accès dans un environnement numérique exige que l'on utilise les ressources de la technologie pour faciliter le repérage et l'extraction des documents souhaités. Dans le même temps, ce droit à la transparence se heurte au droit à la vie privée des personnes visées par ces documents. La question jusqu'ici peu évoquée risque en effet, précisément à cause de l'utilisation des ressources de la technologie de devenir dans le futur proche une question majeure. En effet, il est aisé via l'interrogation sur base d'un nom propre comme mot-clé, de balayer aisément des millions de caractères et donc de documents, pour recomposer immédiatement et de façon précise les caractéristiques, les faits et gestes, l'environnement de cette personne. Le droit de recherche même dans des archives mortes trouve certainement là une de ses limites.

4. La première question est centrale pour la réalisation de l'archivage proprement dit (I). Les deux autres questions sont relatives à la question de l'utilisation des archives (II).

I. Les conditions de réalisation d'un archivage « fiable » dans un environnement électronique

5. Les conditions sine qua non d'une conservation fiable concernent tant le support que le contenu d'un document électronique. La norme ISO 15489 définit le document fiable comme « le document dont le contenu peut être considéré comme la représentation complète et exacte des opérations, des activités ou des faits qu'elles attestent, et sur lequel on peut s'appuyer lors d'opérations ; d'activités ou de faits ultérieurs ».

A. La pérennité du support

6. Sans doute, cette fiabilité du document exige non point la pérennité des supports, ce qui nous l'avons dit est impensable au vu de l'évolution des technologies. Qui peut garantir que les bandes magnétiques, les disquettes actuellement utilisées comme support seront encore

actuels, malgré leur longue période d'utilisation (T. Lieutenant et S. Marin, Archivage et horodatage de documents électroniques, Mai 2000, document disponible sur le site du CRID http://www.crid.be à la rubrique e justice : « documents disponibles ».

[7] Cf. à ce propos le remarquable dossier publié par le Monde interactif, le 14 mars 2001 disponible sur le site http: //interactif.lemonde.fr

demain lisibles demain ? Elle exige cependant leur bonne conservation[8] et, nécessairement, la regénération des supports ou plutôt la migration vers des nouveaux supports lorsque cette régénération ou migration s'imposent[9].

B. La pérennité de la lisibilité

7. Au-delà de ce premier point, comment garantir la lisibilité pérenne des informations contenues sur le support[10]. La question concerne tant le format d'encodage du document (par ex. Word 6, XML ou TIFF) les logiciels en mesure de décoder le format et le matériel informatique permettant de faire fonctionner un tel logiciel. Les risques d'illisibilité sont en effet évidents.

Même si les supports sont bien traités, le logiciel ayant servi à générer les données stockées peut poser problème. En effet, la plus parfaite des conservations de matériel ne servirait à rien s'il est devenu impossible de lire les informations stockées sur le support.

L'évolution permanente des programmes de traitement de données (lecture, ...) et donc leur obsolescence continuelle pose le risque de ne plus pouvoir ouvrir certains fichiers. Citons comme simple exemple Microsoft et son traitement de texte dont les dernières moutures semblent « oublier » les formats précédents de document !

Toutefois, un support impeccable et une application de lecture compatible aux données numériques concernées ne suffisent pas. Il est en effet nécessaire de disposer du système supportant l 'application de lecture : le système d'exploitation. En effet, tout qui a déjà utilisé un ordinateur sait que tel logiciel fonctionnant sur un « Mac » ne peut fonctionner sous Windows, et vice-versa, à moins de disposer de versions spécifiques. Au sein même du

---

[8] « La réponse au problème de la conservation est fondamentalement la même que celle apportée aux risques inhérents au stockage de papier, lequel doit également être préservé du feu, de l'humidité, etc. Les supports sensibles de stockage électronique sont ainsi confinés dans des armoires ignifugés, maintenues à température et humidité constantes, avec l'énorme avantage du gain en volume à sécuriser.
A une échelle plus restreinte, une disquette « archivée » pourra par exemple être conditionnée hermétiquement, garantissant une durée de conservation plus grande qu'une disquette posée sur un coin de bureau.
En ce qui concerne le problème de la dégradation des performances d'une bande magnétique non utilisée, une simple re-lecture/ré-écriture régulière des informations permettra une remagnétisation des particules magnétiques composant la surface du support. Ce dernier problème met en évidence un nouvel enjeu pour l'archivage électronique (qui n'existait pas pour l'archivage classique » (T. Lieutenant et S. Marin, article cité). Sur tout cela, lire également M. Antoine, M. Eloy, JF Brakeland, Le droit de la preuve face aux nouvelles technologies de l'information, Cahier du CRID n° 7, Story Scientia, 1991, p. 129 et s.

[9] Sur les conditions de cette migration, cf. la recommandation déjà ancienne du Conseil de l'Europe (n° R(81)20) qui fixe les conditions techniques mais également procédurales et organisationnelles de cette migration des supports, en particulier, l'opération doit se faire sous la supervision d'un responsable qui devra s'assurer du bon déroulement des opérations, de l'emploi des bonnes techniques garantissant la modification « irréversible » du support et programmes de lectures et d'écriture et signera un protocole qui restera annexé au document ainsi produit. Une solution technique semble se dégager avec les disques WORM (« Write One Read Many), « supports optiques pour lesquels l'écriture des bits codant les données se fait par transformation irréversible d'un ou de plusieurs constituants de ce support » (définition donnée par la norme française NF Z 42-013 : Archivage électronique est une liste de spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des données stockées dans ces systèmes. C'est une norme française homologuée par décision du directeur général d'AFNOR le 20 novembre 2001 pour prendre effet le 20 décembre 2000. La norme selon son préambule « fournit un ensemble de spécifications concernant les mesures techniques et organisations d'aide à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques afin d'assurer la conservation et l'intégrité de ceux-ci ».

[10] Sur cette distinction entre la "durabilité" du contenant et du support, lire M. Demoulin, « La notion de support dans les contrats à distance : une contrefaçon de l'écrit? », Rev. eur. dr. cons. , 4/2000, pp. 361-377.

monde Windows, il arrive que des applications écrites pour la version personnelle, Windows9x ou ME, soient incompatibles avec la version plus professionnelle, NT ou 2000.

8. Trois solutions sont envisageables. JF Blanchette[11] les résume comme suit : « Deux regroupements issus de l'industrie ont tenté de la résoudre : le groupe de standardisation EESSI – chargé du développement de spécifications techniques conformes à la définition de la Directive européenne de « signature électronique avancée » - a proposé la resignature(1), et le développement de services centralisés d'archivage (2), alors que le consortium W3C, dans le cadre du développement de la norme XML, propose l'utilisation (3) de formats de documents dits « canoniques» ».

Cette troisième solution semble l'emporter. L'idée est l'adoption de formats permettant d'archiver le message indépendamment du logiciel de traitement et de l'environnement informatique choisi lors de la création du document[12]. Il va de soi qu'à terme, il faut envisager la généralisation de l'utilisation de ces formats dès la création des messages et documents[13].

C. L'intégrité du document

9. Garantir la lisibilité n'est point suffisant. Il faut encore garantir l'intégrité du document. Le fait que la lisibilité du document soit conservée à travers le temps n'empêche pas qu'il soit un moment donné modifié ou attribué à un autre auteur que son émetteur d'origine. Une loi québécoise définit l'intégrité d'un document comme assurée « lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégrité et que le support qui porte cette information lui procure la stabilité et la pérennité voulue[14]. Il est à noter que selon l'article 6 de cette loi, l'intégrité doit être établie à tout moment du cycle de vie du document depuis sa création jusqu'à l'archivage. Elle peut être assurée par tout

---

[11] JF Blanchette, Signature cryptographique et archivage électronique, document non publié, réalisé dans le cadre de l'étude effectuée par le CECOJI/CNRS (27, rue P. Bert, 94204 IVRY-sur-Seine, France) pour le gouvernement français. Sur ces solutions, lire également D. Bearman, Reality and Chimeras in the Preservation of Electronic Records, D-Lib. Magazine, avril 99, 5 (4) disponible à http: // www.dlib.org/delib/april99/bearman/04bearman:html et F. Boudrez, Het digitale archiveringssysteem, Etude menée dans le cadre du projet DAVID, juin 2001, disponible à l'adresse : http://www.dema.be/david/index2.htm).

[12] Th. Piette-Coudol (Conservation et archivage de l'écrit sous forme électronique, Chron. Jclasseur – Commerce électronique, Mai 2002, p.11) décrit ainsi les différents formats EDIFACT (ISO 9735), SGML (NFEN 28879), et le mode texte ISO/CEI8559 et 10.646. La récente prise de conscience de ce problème de la pérennité de lisibilité des documents a conduit l'association française Aristote (composée de grands organismes de recherche : CNES, CEA, INRIA, ...) à créer en juin 2000, le groupe de réflexion PIN (Pérennisation des informations) dont le but est la conception de formats d'archives universels et impérissables à l'aide du standard XML. XML pour eXtensible Markup Language est un format de description de données qui reprend le principe des balises d'HTML, mais en y ajoutant une grande souplesse, au contraire de son aîné. Si les balises HTML sont fixées par un organisme de normalisation (W3C), chacune est libre de créer son propre descripteur XML. En effet, chaque document XML d'un document DDT reprend la sémantique des balises utilisées. Ainsi, nous retrouvons avec de simples fichiers texte, donc normalement interprétables facilement, qu'il suffit alors de corréler pour exploiter les informations qui y sont stockées. Le DDT est en quelque sorte la clé d'interprétation du XML.

[13] C'est l'idée du gouvernement belge de généraliser l'utilisation des formats XML dans l'administration, ce qui permettra une plus grande circulation de l'information en son sein peu importe les environnements applicatifs et informatiques de chaque administration.

[14] Loi du Québec n° 161 concernant le cadre juridique des technologies de l'information, 21/06/2001 (2ème session 36e lég, 2001, Chap. 32) disponible sur le site www.publicationduquebecge.ca. Cf. également la norme française NF 242-013 qui définit l'intégrité comme la caractéristique d'un document électronique qui n'a subi aucune destruction, altération ou modification ».

moyen. Elle le sera souvent en matière de document électronique par la signature électronique.

Cette signature peut avoir été apposée sur le document lui-même, ainsi le message électronique signé par tel fonctionnaire ou tel juge, message dont on souhaite l'archivage ou être apposée par la suite pour authentifier un document papier qu'on aura souhaité archiver électroniquement ou un document électronique non signé (ex. des publications statistiques). La signature électronique apposée assure, à certaines conditions réglementaires strictes[15], de l'identité du signataire et de l'intégrité du document. Elle joue donc un rôle essentiel pour garantir l'intégrité des archives[16]. « Force est de constater que ce n'est plus le support (originaire) qui assure l'indispensable maintien de l'intégrité mais la signature dont le mécanisme permet de figer logiquement le contenu de l'écrit »[17].

10. Si la signature est donc garantie d'intégrité du contenu, son utilisation soulève cependant un problème. En effet, les processus de migration qui permettent d'assurer la lisibilité pérenne des documents mettent à mal les signatures cryptographiques qui y sont associées. Dans cette mesure, la vérification de la signature n'est plus possible. Bref, l'archivage des signatures cryptographiques crée un dilemme : assurer l'intelligibilité du document oblige à invalider la signature attachée ou garder le moyen de vérifier la signature mais alors le document deviendra inintelligible[18].

Des solutions sont proposées. La première invite à une signature du document. C'est la solution préconisée par le groupe EESSI de l'ETSI[19] qui définit un format de signature, dit ES-A. Il s'agit lorsque la vérification de la signature doit s'opérer à long terme – et c'est le cas qui nous occupe – de collecter selon une structure donnée toutes les informations permettant la vérification future (document original, signature de base, clés, certificat, liste de révocation). Cet ensemble est alors renseigné.

Ce mécanisme de régénération des signatures nécessité l'intervention d'un tiers habilité à procéder à cette « resignature » et un système d'horodatage permettant de fixer le moment de l'opération dont on conçoit l'intérêt : ainsi, une signature dont la sécurité est devenue faible (par exemple, au vu de la longueur de la clé) peut être régénérée avec une clé plus longue mais là s'arrête l'intérêt de l'opération classique puisque la signature originaire est perdue et que la question de base, celle de l'impact de la migration des documents n'est pas résolue.

11. La deuxième solution résulte de la création d'un « service d'archivage centralisé », sorte de TTP (Trusted Third Party) ou pour être plus précis de T.A.S (Trusted Archival Services)[20].

---

[15] Cf. à ce propos, les exigences de la directive européenne 1999/93/CE (JOCE/L.13/12, 19/01/2000) sur la signature électronique du 13 décembre 1999, traduite en droit belge par la loi du 20 octobre 2000 et la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, M.B. 29 septembre 2001, à paraître.

[16] Sur ce role, S. van den Eynde et J. Dumortier, De rol van de digitale handtekening bij het archiveren van elektronische documenten, Bibliotheek en archiefgids, 77(2001) p. 1 et s. Cf. également, M. Demoulin, Conservation et datation des documents électroniques, in Rapport du Groupe IV, document établi dans le cadre des travaux de e-justice, disponible sur le site du CRID à l'adresse déjà indiquée.

[17] D. Gobert et E. Montero, L'ouverture de la preuve littérale aux écrits sous forme électronique, JT 2001, p. 114-128.

[18] Sur ce dilemme, JF Blanchette, art. cité. La description des solutions est largement inspirée de cet auteur.

[19] A cet égard, EESSI, Electronic Signature formats, ETSI, TS 101-733 (version 1.2.2.) disponible à http://www.etsi.org/SEC/ts_101733v.010202p.pdf. Sur ce procédé, lire S. van den Eynde, ...

[20] Selon le terme utilise par le rapport de l'EESSI, Trusted Archival Services, 28 août 2000, p. 2.

Il s'agirait de manière centralisée[21] soit de maintenir une sorte de vaste banque de données permettant de réémuler l'ensemble des signatures[22] ou, de manière plus modeste, en tout cas de conserver en un lieu unique l'ensemble des certificats y compris la mention des clés publiques de manière à pouvoir garantir l'authenticité d'un document et ce bien après sa création. On peut imaginer que le service des Archives joue ce rôle ou émette les normes de qualité voire agrée les services opérant comme T.A.S.

On conçoit la difficulté de cette seconde solution qui oblige, en tout cas, à obtenir la liste de l'ensemble des certificats et des clés publiques, leur date d'émission et de révocation. Si la solution permet la conservation des signatures originaires, elle n'apporte cependant point de solution au problème de la migration soulevée plus haut sauf à considérer que cette migration concernera le message en clair auquel sont apposées les seules informations permettant de l'authentifier et non le message crypté.

12. La troisième solution est celle dite des « formats canoniques » proposé par le consortium W3C[23], dans le cadre de ses travaux visant l'intégration des signatures cryptographiques au langage XML[24]. JF. Blanchette la décrit comme suit :

« Le concept de 'format canonique' consiste ainsi à effectuer une migration du fichier vers un format plus stable, avant même la signature, en espérant ainsi réduire un peu les effets néfastes de l'obsolescence. La spécification XML canonique impose ainsi l'utilisation de l'encodage de caractères UTF-8, encodage qui effectue un pont entre la norme actuelle ASCII (américaine) et les futures normes UNICODE et UCS (plus universelles). En imposant ce pré-traitement, les documents XML seront moins vulnérables à une simple transformation du format d'encodage, tranformation transparente à l'utilisateur, mais qui invaliderait immédiatement la signature. Comme discuté ci-haut, les institutions d'archivage ne font rien d'autre quand elles migrent des formats peu utilisés vers des formats plus communs, réduisant ainsi le nombre de formats d'encodage dont elles doivent assurer la lisibilité. Cependant, la migration vers un format canonique ne résout en rien le problème fondamental : le document signé, canonique ou pas, n'est plus susceptible d'être migré sans détruire les signatures cryptograhiques associées.

13. En conclusion, un archivage « sécurisé » reposera sur les garanties procédurales et techniques qu'à chaque phase de transfert du document, à chaque modification de son

---

[21] Les prestataires de service de certification doivent en toute hypothèse selon la directive européenne conserver les certificats émis pendant cinq ans au moins après l'expiration des clés. La question posée est donc le transfert au-delà de ce terme de l'information relative aux certificats ainsi conservée. A noter sur ce point, la norme X509 de l'UIT qui dans son document « Politique de certification » décrit les tâches du certificateur qui a émis les clés et l'astreint à une « journalisation » et archivage des événements relatif à un certificat. Cf. également en ce sens, le point K) de l'article 6 du décret français 2001-272 du 30 mars pris en application de l'article 1316-4 du Code civil et relatif à la signature électronique. Le certificateur doit « conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique, qui pourraient s'avérer nécessaire pour faire la preuve en justice de la certification électronique ».

[22] "Les opérateurs doivent maintenir un ensemble d'applications (logiciels de visualisation) de même que les logiciels de validation de signature) de même que les plate-formes informatiques correspondants ou au moins la capacité d'émuler de tels logiciels, de façon à garantir que le contenu des documents puisse être lu et que la signature sur ces documents puisse toujours être validée plusieurs années plus tard.

[23] Il s'agit d'un organisme privé d'autorégulation d'Internet, cherchant à spécifier et à promouvoir les normes des services Web d'Internet.

[24] Lire en particulier la description du système in W3C, Canonical XML, version 1.0. (15 mars 2001) disponible sur http : //www.w3org/TR/2001/REC-xml.C14n-20010315.

support, il puisse être démontré que le document résultant comporte la même information que le document source et que son intégrité est assurée. Cette exigence peut être rencontrée

1. par une responsabilisation des « archiveurs », c'est-à-dire des personnes chargées des opérations permettant la conservation à terme des documents.
2. par une recommandation relative à chaque transfert permettant la « traçabilité » des diverses opérations ayant été effectuées et garantissant le maintien de l'intégrité du document[25].
3. par la définition des normes adéquates permettant de guider d'une part, les transmetteurs d'informations c'est-à-dire l'ensemble des administrations et institutions chargées ou désirant transmettre de l'information aux Archives et, d'autre part, les services d'archivage eux-même lors des opérations portant sur les documents à conserver.

II. Principes et limites de l'accessibilité aux données archivées

14. La recommandation n° R(2000)13 établit en son article 3 que : « La législation et la réglementation relatives à la communication des archives publiques devraient être coordonnées et harmonisées avec les lois relatives aux domaines connexes, en particulier avec celle sur l'accès à l'information détenue par les autorités publiques et celle sur la protection des données.

Le premier type de législation énoncé, celui sur l'accès à l'information, fonde une politique d'ouverture large des archives que la protection des données personnelles, objet du second type de législation vient limiter. Comme le note la même recommandation « Des exceptions à cette règle générale, nécessaires dans une société démocratique, peuvent le cas échéant être prévues pour assurer la protection[26] .... b. des particuliers contre la divulgation de données relatives à leur vie privée ».

A. Le principe : le droit d'accès aux archives publiques

15. Les recommandations européennes 5 et 6 établissent clairement que « l'accès aux archives publiques constitue un droit » qui doit être reconnu à tous les utilisateurs et susceptibles d'être exercée gratuitement.

L'utilisation des technologies de l'information et de la communication facilite, nous l'avons dit, l'exploitabilité des documents archivés, en même temps que leur communication. Il est dès lors légitime de souhaiter que les utilisateurs puissent bénéficier des avantages de ces technologies nouvelles. Comme l'écrit Madame C. de Terwangne[27] « il convient d'envisager

[25] Sur cette exigence de traçabilité, les remarques importantes de Th. Piette-Coudol, art. cité., p. 14 et les nombreuses références faites à la loi québécoise n° 161, déjà citée qui, par exemple, requiert (article 30) que la documentation établissant la capacité d'un mode de transmission d'en préserver l'intégrité doit être disponible pour production et preuve, le cas échéant. (Cf. également l'article 21).

[26] La première exception mentionnée par le texte et non reprise ici vise « les intérêts publics prépondérants dignes de protection (tels que la défense nationale, la politique étrangère et l'ordre public) ; »

[27] C. de Terwangne, Société de l'information et mission publique d'information, Thèse défendue à Namur, mars 2001, à paraître in Cahier du CRID. A propos de cette nécessité d'une évolution du service public

la mission publique d'information dans sa juste dimension et d'intégrer au produit d'information la valeur ajoutée qui permettra de satisfaire pleinement le besoin légitime d'information. On ne peut plus, de nos jours, proclamer que la seule réponse adéquate est celle du papier et qu'une mise à disposition par la voie électronique est à considérer comme un débordement commercialisable de la mission de service public. La loi de mutabilité du service public impose d'adapter celui-ci en fonction de l'évolution du contexte notamment technologique ».

Cette nécessité d'une utilisation des nouveaux médias par les archives publiques pour la diffusion des documents collectés ou des résultats de leur analyse a été clairement reconnue par de nombreuses institutions d'Archives publics. Les sites Web que ces institutions ont développés reprennent nombre de documents, d'études ou de synthèses précieuses pour l'utilisateur.

Au-delà, on peut songer à l'obligation de rendre accessible par voie électronique la copie de certains documents archivés. A cet égard, la loi américaine dite « Electronic Freedom of Information »[28] oblige l'administration sollicitée plus de trois fois pour le même document à mettre ce document sur un support électronique et à le rendre accessible via un accès électronique.

Enfin, l'accessibilité par voie électronique suppose une indexation claire des documents[29] et la possibilité pour l'utilisateur d'exploiter les ressources des logiciels d'interrogation dont dispose l'administration des Archives elle-même.

B. L'exception : la protection des données personnelles

16. L'article 22 de l'avant-projet de loi relative aux Archives en discussion au moment de la conférence prévoit que « Par dérogation aux dispositions du paragraphe 1°, les archives publiques ne peuvent être consultées qu'à l'expiration d'un délai de :

> cinquante ans à compter de la date du décès de la personne concernée pour des documents comportant des renseignements individuels à caractère médical ;
> cinquante ans à compter de la date du décès de la personne concernée pour les dossiers relatifs au personnel ou ayant trait à la vie privée.

Ce type de dispositions soulève nombre de difficultés : les unes d'ordre politique dans la mesure où elles supposent un lourd travail d'identification du délai prévu et nécessitent l'identification dans les documents archivés, des données à caractère personnel ; de manière à les occulter le cas échéant ; les autres concernent l'extension des termes choisis. Que veut dire : « renseignement individuel à caractère médical » alors même que la loi du 8 décembre 1992 dite loi vie privée[30] par des données relatives à la santé ? Même question à propos des termes : « dossiers relatifs au personnel ou ayant trait à la vie privée ». Faut-il opposer les

---

informationnel, lire également Yves Poullet, Diffusion des données juridiques et nouveaux médias : un enjeu fondamental pour la justice, in L'information juridique : contenu, accessibilité et circulation, Actes du Congrès de l'ADIJ, Paris 22 et 23 octobre 1998.

[28] Electronic Freedom of Information Act Amendments of 1996.

[29] A cet égard, on note les efforts au sein du Groupe ISO T.C. 96 d'une harmonisation des systèmes de classement et d'interrogation.

[30] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement des données à caractère personnel (M.B., 18 mars 1993) modifiée par la loi du 11 décembre 1998.

mots « dossier » et « traitement » et entendre le mot vie privée de manière étroite alors même que la loi de 1992 protège sous le vocable vie privée, toute donnée à caractère personnel[31,32] ?

Quoiqu'il en soit, la disposition laisse clairement entendre que la protection des données personnelles s'éteint au-delà d'une certaine durée après la mort de la personne concernée. Ce caractère automatique de la perte de la protection étonne. En particulier, en matière médicale, ne faut-il, pas dans certains cas exceptionnels, restreindre l'accès même au-delà du délai prescrit lorsque la révélation d'une donnée à caractère personnel relative à une personne décédée, ainsi une donnée relative à une maladie, peut entraîner un dommage à ses descendant.

Par ailleurs, même si seules les données à caractère strictement personnel sont l'objet de cette protection, on peut, me semble-t-il, considérer que l'interrogation tous azimuths de l'ensemble des archives à propos d'une personne encore en vie ou récemment décédée peut constituer une violation grave de la vie privée de cet individu. Les possibilités infinies qu'offrent les ressources des technologies de l'information et de la communication dans l'interrogation rapide de milliers de documents électroniques, créent à cet égard des risques que ne comportait pas la consultation patiente et tâtonnante des documents papiers. A cet égard, ne faut-il pas interdire ou limiter sévèrement la recherche automatisée sur base de mots clés identifiant des individus ?

18. L'avant-projet de loi prévoit même pour les données personnelles exceptées d'un accès immédiat, la possibilité de leur consultation à des fins de recherche administratives ou scientifiques[33]. Un arrêté royal sera émis à ce propos.

A cet égard, on s'étonne que dans l'avant-projet de loi la recherche administrative soit mise sur le même pied que celle scientifique. Cette assimilation apparaît cependant peu fondée. On sait que l'article 4 de la loi de 1992, telle que modifiée par la loi de 1998, prévoit « qu'un traitement ultérieur à des fins historiques, statistiques ou scientifiques n'est pas réputé incompatible lorsqu'il est effectué conformément aux conditions fixées par le Roi « qui

---

[31] Sur ces diverses notions, lire Th. Léonard, Y. Poullet, La protection des données à caractère personnel en pleine (r)évolution : la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995, J.T., 1999, p. 377 et s. La Commission de protection de la vie privée dans son avis n° 49/2001 du 10 décembre 2001 relatif à cet avant-projet réclame également une plus grande clarté (avis disponible sur le site de la Commission (http : ww.privacy.fgov.be) : « Aux termes de l'article 22 du projet, les archives doivent avoir au moins 30 ans avant de pouvoir être consultées. Ce délai est porté à 50 ans lorsque la sûreté de l'Etat est menacée et à 100 ans lorsqu'elles contiennent évidemment de ce qu'il y a lieu d'entendre par « informations concernant la vie privée ». Si elles désignent toutes les données à caractère personnel au sens de la LVP, ce projet de loi ne contient aucun assouplissement par rapport aux dispositions de la loi relative aux archives étant des « données à caractère personnel sensibles », à savoir les données à caractère personnel concernant la vie sexuelle (article 6 LVP), la santé (article 7 LVP), les litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives, des suspicions, des poursuites ou des condamnations (article 8 de la loi relative à la protection de la vie privée). D'autres catégories de données à caractère personnel jugées sensibles pourraient y être ajoutées. A noter que la LVP lève la protection particulière de ces données lorsque leur traitement est nécessaire à la recherche scientifique ou lorsqu'elles ont été manifestement rendues publiques par la personne concernée (cette dernière éventualité est exclue pour des données à caractère personnel judiciaires). Dans ce cas, elles ne doivent plus être considérées comme sensibles. Pour lever le moindre doute, le projet de loi devrait reprendre la terminologie de la LVP s'il considère que certaines données à caractère personnel doivent bénéficier d'un délai supplémentaire avant de pouvoir être rendues accessibles ».

[32] A noter que la Commission s'était déjà prononcée antérieurement sur des projets ayant le même objet en 1995/avis n° 02/1995) et en 1997 (avis n° 26 et 27/1997).

[33] Cette dérogation est suspendue à la prise d'un arrêté royal après avis de la Commission de Protection de la Vie Privée.

prévoit des garanties appropriées pour les données à caractère personnel qui sont conservées au-delà de la période précitée à des fins historiques ... ».

Sans doute, eût-il été préférable de se référer à cette disposition et à l'arrêté royal pris pour son application. Cet arrêté décrit en effet soigneusement les conditions pour l'utilisation des données à caractère personnel et ce à des fins historiques, scientifiques ou statistiques[34]

Enfin, à propos de ces dérogations, l'exposé des motifs précise qu'elles ne peuvent « en aucun cas (....) porter atteinte à l'intérêt des personnes privées ». Ceci est bien sûr une résolution louable mais formulée de façon si absolue qu'elle n'est pas tenable. Il serait préférable de procéder à une évaluation des intérêts étant entendu que le dommage qui serait éventuellement causé à la personne privée doit être inférieur à l'intérêt plus général de la consultation. Les Archives de l'Etat devraient mettre en place, une cellule chargée de veiller à cette évaluation in *casu* et, plus largement, de garantir le respect de la législation de protection des données.

Conclusion

19. L'adoption par les Archives du Royaume d'une politique d'utilisation de l'électronique dans la production, l'exploitation et la conservation des Archives est une obligation au vu du « tout électronique » vers lequel s'orientent l'Administration et nos sociétés.

Face à cette nécessité, il est indispensable que les Archives, si elles veulent continuer à jouer le rôle de mémoire collective qui est le leur, attirent fortement l'attention des pouvoirs publics sur les conditions dans lesquelles elles pourront jouer le rôle essentiel à nos démocraties. Placées en aval de toutes les opérations, conçues pour la pérennité, les Archives ne peuvent se satisfaire des politiques présentes où technologies modernes riment avec fugacité et volatilité.

Pour répondre au défi du temps, il est indispensable que soit adoptée une politique de normalisation des messages, une standardisation des procédures de création et de conservation des documents électroniques qui permettent d'en garantir à horizon temporel indéfini, la conservation intègre et lisible. Sans doute, cette politique a-t-elle un coût mais les enjeux de cette politique pour les générations à venir sont de taille.

Il importe que les services des Archives soient dès le départ associés à la définition de cette politique et qui, sans doute, une réorganisation de ceux-ci, leur permette d'appréhender correctement les implications des choix technologiques et, avec chaque administration, de définir les politiques de conservation des documents quant au contenu des documents à archiver et quant aux conditions de leur conservation. A cet égard, l'Archivage ne doit plus nécessairement signifier un archivage physiquement localisé en des lieux dédiés mais pourrait parfaitement devenir virtuel, sans déplacement de documents et de supports mais par simple connexion de fichiers préalablement identifiés.

---

[34] Pour l'examen de ces conditions, nous renvoyons le lecteur à l'étude minutieuse proposée par C. de Terwangne, S. Louveaux,, Protection de la vie privée face au traitement de données à caractère personnel : le nouvel arrêté royal, JT du 26 mai 2001, pp. 457-469.

20. Au-delà, nous avons attiré l'attention des lecteur sur quelques éléments qui pourraient aider nos décideurs à trouver le juste équilibre entre, d'une part, les préoccupations légitimes certes de la confidentialité que consacre la loi dite vie privée, et, d'autre part, les exigences de transparence et de débats démocratiques que soulignent les lois sur la publicité des documents administratifs et sur l'archivage. Ne s'agit-il pas en effet, d'enrichir notre vision de la société, en rendant plus facile l'exploration du passé. A cet égard, la pleine utilisation des technologies de l'information et de la communication est un outil précieux, à condition qu'il soit maîtrisé et mis au service d'une politique volontariste de développement des Archives de l'Etat.